HIT Testimony
January 7, 2010

Written Statement of
David C Miller
Chief Security Officer
Covisint Corporation, a Compuware Company

Introduction

Distinguished Members of the HIT Policy Committee I would like to thank you for the opportunity to discuss approaches to authentication within a healthcare context. Given the fact that all types of communication in our country are shifting away from face-to-face in favor of electronic media, it is vital that we consider the alternatives for authentication of those users. This holds particularly true in the healthcare industry where the proper identification of a healthcare professional is paramount to the security and privacy of the patient data.

In the years that I have been working as a security expert at EDS, IBM, General Motors, and now with Covisint Corporation, a Compuware Company, I have become very familiar with the challenges related to authenticating users. The challenge related to user security is much different than that in which we see in securing of infrastructure or transactions. In the later cases the standard can be mandated and is, in most cases, implemented by security professionals. In the former “user access” case the authentication is performed by persons who have little interest or time for complicated, yet secure credentials. This often leads to some very creative workarounds for access if the security authentication method is to onerous. On the other hand, a method that is very simple for the user may also open the system up for unauthorized access. This balance between security and usability is by far the major challenge in all authentication systems.

One deceptively simple approach to simplifying authentication is to minimize the need for it. Simply put, if I can authenticate myself once and then access a myriad of applications I would be very willing to accept a more complicated user access authentication. On the other hand if I am required to manage multiple ID’s and logins I will find ways to simplify my access. My experience is that users want to be secure, but that security must work within their overall work habits.

Another key element is to leverage existing ID's. Does the user authenticate themselves somewhere in the community today, and is there a way that that credential can be leveraged across the community? This allows the trust to be shared across the community and puts it closer to the user.

Covisint has solved this problem by creating "Identity Hub's" for the healthcare industry that allows users a single place to login and manage authentication. This vastly simplifies the work of the user in relation to access and therefore allows us to implement more complex authentication methods. In addition, this single point of user management gives a single point for implementation of administrative systems thus streamlining the provisioning and de-provisioning of users, not to mention reducing overall helpdesk and other support costs. Our implementation also includes a federation hub that allows authentications that occur at the users' location to be shared across the whole community.

In relation to the criteria for the authentication we have determined some evaluation criteria that need to be taken into consideration.

- **Additional Hardware**

  Some of the authentication methods require separate hardware infrastructures - this can cause significant cost and increase complexity. Also don't forget about client hardware requirements.

- **Additional Software**

  This is the same as the hardware issue but is for software. The client case is particularly challenging. For example the ability to store a certificate may require a operating system upgrades. That can lead to additional hardware.

- **Complexity**

  This holds true for both sides of the implementation. The management of path validation in certificates is very complex and the accepting organization my not have sufficient

capability to manage this. You also need to look at the client and user complexity of the system. Is the user required to run or install something that will make it hard for the average user to understand what to do? In addition complexity often comes out in the resolving of problem situations.

- **Scalability**

  Will the solution scale to thousands or millions of users. This related to the running of the solution but also the dissemination of the credential.

- **Portability**

  Will it work on many platforms and systems?

- **Login Time**

  In healthcare this is particularly important. If it takes minuets to login it may not work in critical care situations.

- **Acquisition Costs**

  What is the cost for the license of the technology?

- **Operating Cost**

  This factor is often due to large increases in helpdesk. If the solution is difficult to use and you have thousands of users using it, you may incur very large helpdesk call volume.

Questions:

1) What Trust problems does Covisint solve?

Covisint currently supports various identity hub implementations across the U.S. The largest of these include Minnesota, Tennessee, The American Medical Association (AMA) and three regional hubs in the state of Michigan. Across these communities we support well in excess of 300,000 healthcare professionals access to each of their community resources.

In addition, Covisint supports a Department of Justice (DOJ) implementation that allows local law enforcement access to terrorist information hosted at various federal agencies. This implementation leverages the local authentication of the user.

In these implementations Covisint supports various forms of authentication, which include:

- Password
- Token
- Certificate (including HSPD12 issued certificates)
- Grid card-based

In these implementations Covisint also supports both delegated and Knowledge-based (KBA) provisioning methods.

2) Who pays?

Ultimately, the organization that derives the benefit from the identities access pays for the ID management. In many cases that is the community owner, the state, health information exchange (HIE), or healthcare organization. In some instances the derived benefit is the reduction of cost and complexity created by having to manage the authentication on their own.

Cost is based on the complexity of the authentication method (certificates are more complex to manage then passwords) and the requirement for a level-one help desk. In many cases the helpdesk cost is by far the largest and least predictable.

3) How can one deal with certificates as access?

Certificates can create a special problem for access. This is because the technologies required to manage the validation of a certificate can be complex and costly. By intermediating between the certificate and the resource we have found you can reduce total complexity and cost for the whole community.

This is the strategy for the DOJ implementation. We accept the certificate as authentication and then translate that into a standard federation protocol for consumption by the end service.

4) What about Delegated Administration?

The first thing we have learned is that delegated administration is not the only manner of administration that should be supported. The Knowledge-based administration (KBA) in which the user answers a set of questions to validate themselves is also a valid method of administration. We are currently working with the AMA to define an appropriate set of KBA information that can be used by healthcare professionals for validation of access.

Covisint support both of these methods thus allowing a community to pick the type that best suits them. It also allows for the mixing of administration methods for an individual user. Perhaps KBA will allow a lower level access then delegated administration would.

5) What role can the government take?

Ultimately, the role of the government is to define an acceptable standard for authentication to various healthcare resources. This standard then can be implemented by third parties such as Covisint. The challenge is to accept some of the weaker forms of authentication (password) for access to some data while choosing a menu of higher level authentications for more secure access. The current NIST standard (SP800-63) requires the most complex implementation scenarios for access thus creating an environment that does not encourage adoption of the standard.

This exact problem is being seen today in relation to the e-prescribing authentication standard that is being proposed by the DEA. This standard required such a high- level of authentication that it makes it very challenging for most organizations to implement.

By applying the previously mentioned rating criteria we believe that an implementable standard can be proposed. We also believe that giving various options for authentication will allow organizations the freedom to choose solutions that fit into their architectures.

We also feel that the support of Identity Hubs through defined interoperability standards will allow communities to implement faster then if the direction is for each organization to implement there own interface.

Conclusion

Ultimately, the success of any system is all about adoption. Getting the constituents to adopt a new methodology will require selection of a cost-effective, simple and secure solution. We believe that there are simple-to-use technologies, which--when partnered with policy and oversight--can achieve adoption within the whole healthcare community. This approach can also overcome the concerns associated with enabling a complex authentication system. I have seen this approach work successfully in many industries over the past seven years and believe it has real merit and deserves further consideration.

Members of the Committee, I thank you for the opportunity to discuss this vital issue and welcome any questions you may have.